A Robust Specification Theory for Modal Event-Clock Automata

Uli Fahrenberg, Axel Legay

A Robust Specification Theory for Modal Event-Clock Automata

Uli Fahrenberg Axel Legay
Irisa / INRIA
Rennes, France

In a series of recent work, we have introduced a general framework for quantitative reasoning in specification theories. The contribution of this paper is to show how this framework can be applied to yield a robust specification theory for timed specifications.

1 Introduction

Specification theories allow to reason about behaviors of systems at the abstract level, which is needed in various application such as abstraction-based model checking for programming languages, or compositional reasoning. Depending on the application for which they are used, such specification theories may come together with (1) a satisfaction relation that allows to decide whether an implementation is a model of the specification, (2) a notion of refinement for determining the relationship between specifications and their set of implementations, (3) a structural composition which at the abstract level mimics the behavioral composition of systems, (4) a quotient that allows to synthesize specifications from refinements, and (5) a logical composition that allows to compute intersections of sets of implementations, *cf.* [2].

Prominent among existing specification theories, outside logics, is the one of *modal transition systems* [6, 14–16, 19, 22, 23] which are labeled transition systems equipped with two types of transitions: *must* transitions that are mandatory for any implementation, and *may* transitions which are optional for an implementation. So far, existing modal specification theories have relied on Boolean versions of both the refinement and the satisfaction relation. They are hence *fragile* in the sense that they are unable to quantify the impact of small variations of the behavior of the environment in which a component is working. In a series of recent work [3–5], and building on a general theory of quantitative analysis of systems [10, 11, 13, 20, 26], we have leveraged this problem by extending modal specifications from the Boolean to the quantitative world and introducing truly quantitative versions of the operators mentioned above.

The contribution of this paper is to show how our general quantitative framework from [4] can be used to define a notion of robustness for timed modal specifications, or model event-clock specifications (MECS) [7]. We first observe that the notion of refinement proposed in [7] is not adequate to reason on MECS in a robust manner. We then propose a new version of refinement that can capture quantitative phenomena in a realistic manner, and proceed to exhibit the properties of the above specification-theory operators with respect to this quantitative refinement. We show that structural composition and quotient have properties which are useful generalizations of their standard Boolean properties, hence they can be employed for robust reasoning on MECS without problem. Conjunction, on the other hand, is generally not robust (similarly to the problems exposed in [3]), but together with the new operator of quantitative widening can be used in a robust manner.

Preliminary Report. Final version to appear in:
FIT 2012

2 Quantitative Specification Theories

General quantitative specification theories have been introduced in [4]. These consist of

- a specification formalism: modal transition systems with labels drawn from a set Spec,
- a distance on traces of labels: $d_T : \mathsf{Spec} \times \mathsf{Spec} \to \mathbb{R}_{\geq 0}$, and
- operations on specifications which allow high-level reasoning and which generally are continuous with respect to the natural distance on specifications induced by the trace distance.

Below we give a more detailed account of these things, in order to be able to apply them to modal event-clock specifications later.

2.1 Structured Modal Transition Systems

We assume that the set Spec of labels comes with a partial order $\sqsubseteq_{\mathsf{Spec}}$ modeling *refinement* of data: if $k \sqsubseteq_{\mathsf{Spec}} \ell$, then k is more refined (leaves fewer choices) than ℓ. The set $\mathsf{Imp} = \{k \in \mathsf{Spec} \mid k' \sqsubseteq_{\mathsf{Spec}} k \Longrightarrow k' = k\}$ is called the set of *implementation labels*; these are the data which cannot be refined further.

We let $[\![k]\!] = \{k' \in \mathsf{Imp} \mid k' \sqsubseteq k\}$ denote the set of implementation refinements of a label k, and we assume that Spec is well-formed in the sense that $[\![k]\!] \neq \emptyset$ for all $k \in \mathsf{Spec}$: any specification label can be implemented.

A *structured modal transition system* (SMTS) is a tuple $(S, s_0, \dashrightarrow_S, \longrightarrow_S)$ consisting of a set S of states, an initial state $s_0 \in S$, and *must* and *may* transitions $\longrightarrow_S, \dashrightarrow_S \subseteq S \times \mathsf{Spec} \times S$ for which it holds that for all $s \xrightarrow{k}_S s'$ there is $s \overset{\ell}{\dashrightarrow}_S s'$ with $k \sqsubseteq_{\mathsf{Spec}} \ell$. This last condition is one of *consistency*: everything which is required, is also allowed.

An SMTS $(S, s_0, \dashrightarrow_S, \longrightarrow_S)$ is an *implementation* if $\longrightarrow_S = \dashrightarrow_S \subseteq S \times \mathsf{Imp} \times S$, *i.e.* an ordinary labeled transition system with labels in Imp. Hence in an implementation, all optional behavior has been resolved, and all data has been refined to implementation labels.

A *modal refinement* of SMTS S, T is a relation $R \subseteq S \times T$ such that for any $(s,t) \in R$,

- whenever $s \overset{k}{\dashrightarrow}_S s'$, then also $t \overset{\ell}{\dashrightarrow}_T t'$ for some $k \sqsubseteq_{\mathsf{Spec}} \ell$ and $(s',t') \in R$,
- whenever $t \xrightarrow{\ell}_T t'$, then also $s \xrightarrow{k}_S s'$ for some $k \sqsubseteq_{\mathsf{Spec}} \ell$ and $(s',t') \in R$.

Thus any behavior which is permitted in S is also permitted in T, and any behavior required in T is also required in S. We write $S \leq_m T$ if there is a modal refinement $R \subseteq S \times T$ with $(s_0,t_0) \in R$, and $S \equiv_m T$ if there is a two-sided refinement $S \leq_m T$ and $T \leq_m S$.

The *implementation semantics* of a SMTS S is the set $[\![S]\!] = \{I \leq_m S \mid I \text{ is an implementation}\}$, and we write $S \leq_t T$ if $[\![S]\!] \subseteq [\![T]\!]$, saying that S thoroughly refines T.

2.2 Distances

The above setting is purely *qualitative*, *i.e.* Boolean: a refinement $S \leq_m T$ either holds, or it does not; a transition system I either is an implementation of a specification S, or it is not. In order to turn this setting into a *quantitative* one, where we can reason about *robustness* of refinements and implementations, we need to introduce *distances*.

We have in [11] developed a general framework which allows to reason about a variety of such system distances in a uniform way. To apply this to specifications, let $\mathsf{Spec}^\infty = \mathsf{Spec}^* \cup \mathsf{Spec}^\omega$ denote the set of finite and infinite traces over Spec, and let $d_T : \mathsf{Spec}^\infty \times \mathsf{Spec}^\infty \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ be an extended hemimetric.

Recall that this means that $d_T(\sigma,\sigma)=0$ for all $\sigma\in\mathsf{Spec}^\infty$, and that $d_T(\sigma_1,\sigma_2)+d_T(\sigma_2,\sigma_3)\geq d_T(\sigma_1,\sigma_3)$ for all $\sigma_1,\sigma_2,\sigma_3\in \mathit{Spec}^\infty$. Note that as $\mathsf{Spec}\subseteq\mathsf{Spec}^\infty$, d_T induces a hemimetric on Spec.

Let M be an arbitrary set and $\mathbb{L}=(\mathbb{R}_{\geq 0}\cup\{\infty\})^M$ the set of functions from M to the extended non-negative real line. Then $\mathbb{L}$ is a complete lattice with partial order $\sqsubseteq_\mathbb{L}$ given by $\alpha\sqsubseteq_\mathbb{L}\beta$ if and only if $\alpha(x)\leq\beta(x)$ for all $x\in M$, and with an addition $\oplus_\mathbb{L}$ given by $(\alpha\oplus_\mathbb{L}\beta)(x)=\alpha(x)+\beta(x)$. The bottom element of $\mathbb{L}$ is also the zero of $\oplus_\mathbb{L}$ and given by $\bot_\mathbb{L}(x)=0$, and the top element is $\top_\mathbb{L}(x)=\infty$. We also define a metric on $\mathbb{L}$ by $d_\mathbb{L}(\alpha,\beta)=\sup_{x\in M}|\alpha(x)-\beta(x)|$.

Let $F:\mathsf{Spec}\times\mathsf{Spec}\times\mathbb{L}\to\mathbb{L}$ be a function with the following properties:

- F is continuous in the first two coordinates: $F(\cdot,k,\alpha)$ and $F(k,\cdot,\alpha)$ are continuous functions $\mathsf{Imp}\to\mathbb{L}$ for all $k\in\mathsf{Spec}$, $\alpha\in\mathbb{L}$.
- F is monotone in the third coordinate: $F(k,\ell,\cdot)$ is a monotone function $\mathbb{L}\to\mathbb{L}$ for all $k,\ell\in\mathsf{Spec}$.
- $F(\cdot,\cdot,\bot_\mathbb{L})$ extends d_T: for all $k,\ell\in\mathit{Spec}$, $F(k,\ell,\bot_\mathbb{L})=d_T(k,\ell)$.
- F acts as a Hausdorff metric [21] when specification labels are viewed as sets of implementation labels: for all $k,\ell\in\mathsf{Spec}$ and $\alpha\in\mathbb{L}$, $F(k,\ell,\alpha)=\sup_{m\in[\![k]\!]}\inf_{n\in[\![\ell]\!]}F(m,n,\alpha)$.
- Sets of implementation labels are closed with respect to F: for all $k,\ell\in\mathsf{Spec}$ and $\alpha\in\mathbb{L}$ with $F(k,\ell,\alpha)\neq\top_\mathbb{L}$, there are $m\in[\![k]\!]$, $n\in[\![\ell]\!]$ with $F(m,\ell,\alpha)=F(k,n,\alpha)=F(k,\ell,\alpha)$.
- F satisfies an extended triangle inequality: for all $k,\ell,m\in\mathsf{Spec}$ and $\alpha,\beta\in\mathbb{L}$, $F(k,\ell,\alpha)\oplus_\mathbb{L}F(\ell,m,\beta)\sqsupseteq_\mathbb{L}F(k,m,\alpha\oplus_\mathbb{L}\beta)$.

As the last ingredients, let $h_T:\mathsf{Spec}^\infty\times\mathsf{Spec}^\infty\to\mathbb{L}$ and $g:\mathbb{L}\to\mathbb{R}_{\geq 0}\cup\{\infty\}$ be functions such that g is monotone with $g(\bot_\mathbb{L})=0$, $g(\alpha)\neq\infty$ for $\alpha\neq\top_\mathbb{L}$, and $g\circ h_T=d_T$, and such that h_T has a recursive characterization, using F, as follows:

$$h_T(\sigma,\tau)=\begin{cases}F(\sigma_0,\tau_0,h_T(\sigma^1,\tau^1)) & \text{if } \sigma,\tau\neq\varepsilon,\\ \top_\mathbb{L} & \text{if } \sigma=\varepsilon,\tau\neq\varepsilon \text{ or } \sigma\neq\varepsilon,\tau=\varepsilon,\\ \bot_\mathbb{L} & \text{if } \sigma=\tau=\varepsilon.\end{cases}\tag{1}$$

Here $\varepsilon\in\mathsf{Spec}^\infty$ denotes the empty sequence, and for any $\sigma\in\mathsf{Spec}^\infty$, σ_0 denotes its first element and σ^1 the tail of σ with the first element removed.

For technical reasons, we will work mostly with the auxiliary function $h_T:\mathsf{Spec}^\infty\times\mathsf{Spec}^\infty\to\mathbb{L}$ below instead of the distance d_T; indeed, the framework in [4] has been developed completely without reference to the distance d_T which, from a point of view of applications, should be the actual function of interest. This is due to the fact that the recursive characterization in (1) needs to "live" in $\mathbb{L}$ to be applicable to non-trivial distances, *cf.* [11].

We assume all SMTS to be *compactly branching* [9], that is, for any SMTS S and any $s\in S$, the sets $\{k\in\mathsf{Spec}\mid s\overset{k}{\dashrightarrow}s'\}$ and $\{k\in\mathsf{Spec}\mid s\overset{k}{\longrightarrow}s'\}$ are to be compact under the hemimetric d_T. A SMTS S is said to be *deterministic* if it holds for all $s\in S$, $s\overset{k_1}{\dashrightarrow}_S s_1$, $s\overset{k_2}{\dashrightarrow}_S s_2$ for which there is $k\in\mathsf{Spec}$ with $h_T(k,k_1)\neq\top_\mathbb{L}$ and $h_T(k,k_2)\neq\top_\mathbb{L}$ that $k_1=k_2$ and $s_1=s_2$.

2.3 Operations

Any specification theory comes equipped with certain operations which allow high-level reasoning [2]: refinement, structural composition and quotient, and conjunction. For our quantitative framework, we add an operation of *widening* which allows to systematically relax specifications.

The *modal refinement distance* $d_m : S \times T \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ between the states of SMTS S, T is defined using an auxiliary function $h_m : S \times T \to \mathbb{L}$, which in turn is defined to be the least fixed point to the equations

$$h_m(s,t) = \max \begin{cases} \sup\limits_{s \overset{k}{\dashrightarrow}_S s'} \inf\limits_{t \overset{\ell}{\dashrightarrow}_T t'} F(k,\ell,h_m(s',t')), \\ \sup\limits_{t \overset{\ell}{\longrightarrow}_T t'} \inf\limits_{s \overset{k}{\longrightarrow}_S s'} F(k,\ell,h_m(s',t')). \end{cases}$$

We let $d_m = g \circ h_m$, using the function $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ from above. Also, $d_m(S,T) = d_m(s_0,t_0)$, and we write $S \leq_m^\alpha T$ if $d_m(S,T) \sqsubseteq_{\mathbb{L}} \alpha$. This definition is an extension of the one of *simulation distance* in [13], and the proof of existence of the least fixed point is similar to the one in [20]. Note also that d_m extends the refinement relation $\leq_m$ in the sense that $s \leq_m t$ implies $d_m(s,t) = 0$.

The *thorough refinement distance* from an SMTS S to an SMTS T is

$$d_t(S,T) = \sup_{I \in [\![S]\!]} \inf_{J \in [\![T]\!]} d_m(I,J),$$

and we write $S \leq_t^\alpha T$ if $d_t(S,T) \sqsubseteq_{\mathbb{L}} \alpha$. Again, $S \leq_t T$ implies $d_t(S,T) = 0$. It can be shown [4] that both d_m and d_t obey triangle inequalities in the sense that $d_m(S,T) + d_m(T,U) \geq d_m(S,U)$ and $d_t(S,T) + d_t(T,U) \geq d_t(S,U)$ for all SMTS S, T, U. Also, $d_t(S,T) \leq d_m(S,T)$ for all SMTS S, T, and $d_t(S,T) = d_m(S,T)$ if T is deterministic [4].

To introduce *structural composition* and *quotient* of SMTS, one needs corresponding operators on labels. Let thus $\oplus : \mathsf{Spec} \times \mathsf{Spec} \hookrightarrow \mathsf{Spec}$ and $\oslash : \mathsf{Spec} \times \mathsf{Spec} \to \mathsf{Spec}$ be partial label operators which satisfy the following conditions:

- For all $k,\ell,k',\ell' \in \mathsf{Spec}$, if $h_T(k,\ell) \neq \top_{\mathbb{L}}$ and $h_T(k',\ell') \neq \top_{\mathbb{L}}$, then $k \oplus k'$ is defined if and only if $\ell \oplus \ell'$ is defined;
- for all $k,\ell,m \in \mathsf{Spec}$, $\ell \oslash k$ is defined and $m \sqsubseteq_{\mathsf{Spec}} \ell \oslash k$ if and only if $k \oplus m$ is defined and $k \oplus m \sqsubseteq_{\mathsf{Spec}} \ell$;
- for all $\ell,\ell' \in \mathsf{Spec}$, the following conditions are equivalent:
  - there exists $k \in \mathsf{Spec}$ for which both $h_T(k,\ell) \neq \top_{\mathbb{L}}$ and $d_T(k,\ell') \neq \top_{\mathbb{L}}$;
  - there exists $m \in \mathsf{Spec}$ for which both $\ell \oplus m$ and $\ell' \oplus m$ are defined;
  - there exists $m \in \mathsf{Spec}$ for which both $m \oslash \ell$ and $m \oslash \ell'$ are defined.

The *structural composition* of SMTS S, T is then the SMTS $S \| T = (S \times T, (s_0,t_0), \dashrightarrow_{S\|T}, \longrightarrow_{S\|T})$ with transitions defined as follows:

$$\frac{s \overset{k}{\dashrightarrow}_S s' \qquad t \overset{\ell}{\dashrightarrow}_T t' \qquad k \oplus \ell \text{ defined}}{(s,t) \overset{k\oplus\ell}{\dashrightarrow}_{S\|T} (s',t')} \qquad \frac{s \overset{k}{\longrightarrow}_S s' \qquad t \overset{\ell}{\longrightarrow}_T t' \qquad k \oplus \ell \text{ defined}}{(s,t) \overset{k\oplus\ell}{\longrightarrow}_{S\|T} (s',t')}$$

It can be shown [5] that for all SMTS S, S', T, T', $S \leq_m T$ and $S' \leq_m T'$ imply $S\|S' \leq_m T\|T'$. For a quantitative generalization of this, we need a function $P : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ which permits to infer bounds on distances on synchronized labels. We assume that P is monotone in both coordinates, has $P(\bot_{\mathbb{L}},\bot_{\mathbb{L}}) = \bot_{\mathbb{L}}$, $P(\alpha,\top_{\mathbb{L}}) = P(\top_{\mathbb{L}},\alpha) = \top_{\mathbb{L}}$ for all $\alpha \in \mathbb{L}$, and that

$$F(k \oplus k', \ell \oplus \ell', P(\alpha,\alpha')) \sqsubseteq_{\mathbb{L}} P(F(k,\ell,\alpha), F(k',\ell',\alpha'))$$

for all $k,\ell,k',\ell' \in \mathsf{Spec}$ and $\alpha,\alpha' \in \mathbb{L}$ for which $k \oplus k'$ and $\ell \oplus \ell'$ are defined. Then P can be used to bound distances between structural compositions: for SMTS S, T, S', T', we have $h_m(S\|S', T\|T') \sqsubseteq_{\mathbb{L}} P(h_m(S,T), h_m(S',T'))$ [4, Thm. 2].

For the definition of quotient, we first need to introduce *pruning*. For a SMTS S and a subset $B \subseteq S$ of states, the pruning $\rho_B(S)$ is given as follows: Define a *must*-predecessor operator $\mathsf{pre} : 2^S \to 2^S$ by $\mathsf{pre}(S') = \{s \in S \mid \exists k \in \mathsf{Spec}, s' \in S' : s \xrightarrow{k} s'\}$ and let pre^* be the reflexive, transitive closure of pre. Then $\rho_B(S)$ exists if $s_0 \notin \mathsf{pre}^*(B)$, and in that case, $\rho_B(S) = (S_\rho, s_0, \dashrightarrow_\rho, \longrightarrow_\rho)$ with $S_\rho = S \setminus \mathsf{pre}^*(B)$, $\dashrightarrow_\rho = \dashrightarrow \cap (S_\rho \times \mathsf{Spec} \times S_\rho)$, and $\longrightarrow_\rho = \longrightarrow \cap (S_\rho \times \mathsf{Spec} \times S_\rho)$.

The *quotient* of an SMTS T by an SMTS S is the SMTS $T \mathbin{\backslash\!\backslash} S = \rho_B(T \times S \cup \{u\}, (t_0, s_0), \dashrightarrow_{T \backslash\!\backslash S}, \longrightarrow_{T \backslash\!\backslash S})$ given as follows (if it exists):

$$\frac{t \overset{\ell}{\dashrightarrow}_T t' \qquad s \overset{k}{\dashrightarrow}_S s' \qquad \ell \oslash k \text{ defined}}{(t,s) \overset{\ell \oslash k}{\dashrightarrow}_{T \backslash\!\backslash S} (t',s')} \qquad \frac{t \overset{\ell}{\longrightarrow}_T t' \qquad s \overset{k}{\longrightarrow}_S s' \qquad \ell \oslash k \text{ defined}}{(t,s) \overset{\ell \oslash k}{\longrightarrow}_{T \backslash\!\backslash S} (t',s')}$$

$$\frac{t \overset{\ell}{\longrightarrow}_T t' \qquad \forall s \overset{k}{\longrightarrow}_S s' : \ell \oslash k \text{ undefined}}{(t,s) \in B}$$

$$\frac{m \in \mathsf{Spec} \qquad \forall s \overset{k}{\dashrightarrow}_S s' : k \oplus m \text{ undefined}}{(t,s) \overset{m}{\dashrightarrow}_{T \backslash\!\backslash S} u} \qquad \frac{m \in \mathsf{Spec}}{u \overset{m}{\dashrightarrow}_{T \backslash\!\backslash S} u}$$

Note the extra universal state u which is introduced here. The standard property of quotient is as follows [5]: For SMTS S, T, X, for which S is deterministic and $T \mathbin{\backslash\!\backslash} S$ exists, $X \leq_m T \mathbin{\backslash\!\backslash} S$ if and only if $S \| X \leq_m T$. Note that this property implies *uniqueness* (up to $\equiv_m$) of quotient [12]; hence if quotient exists, it must be defined as above.

For quantitative properties of quotient, we must again look to properties of the label operator $\oslash$ which can ensure them. We say that $\oslash$ is *quantitatively well-behaved* if it holds for all $k, \ell, m \in \mathsf{Spec}$ that $\ell \oslash k$ is defined and $h_T(m, \ell \oslash k) \neq \top_{\mathbb{L}}$ if and only if $k \oplus m$ is defined and $d_T(k \oplus m, \ell) \neq \top_{\mathbb{L}}$, and in that case, $F(m, \ell \oslash k, \alpha) \sqsupseteq_{\mathbb{L}} F(k \oplus m, \ell, \alpha)$ for all $\alpha \in \mathbb{L}$. For such a quantitatively well-behaved $\oslash$ it can be shown [4, Thm. 3] that for all SMTS S, T, X such that S is deterministic and $T \mathbin{\backslash\!\backslash} S$ exists, $h_m(X, T \mathbin{\backslash\!\backslash} S) \sqsupseteq_{\mathbb{L}} h_m(S \| X, T)$.

For *conjunction* of SMTS, we need a partial label operator $\owedge : \mathsf{Spec} \times \mathsf{Spec} \to \mathsf{Spec}$ for which it holds that

- for all $k, \ell \in \mathsf{Spec}$, if $k \owedge \ell$ is defined, then $k \owedge \ell \sqsubseteq_{\mathsf{Spec}} k$ and $k \owedge \ell \sqsubseteq_{\mathsf{Spec}} \ell$
- for all $k, \ell, m \in \mathsf{Spec}$ for which $m \sqsubseteq_{\mathsf{Spec}} k$ and $m \sqsubseteq_{\mathsf{Spec}} \ell$, $k \owedge \ell$ is defined and $m \sqsubseteq_{\mathsf{Spec}} k \owedge \ell$, and
- for all $\ell, \ell' \in \mathsf{Spec}$, there exists $k \in \mathsf{Spec}$ for which $h_T(k, \ell) \neq \top_{\mathbb{L}}$ and $h_T(k, \ell') \neq \top_{\mathbb{L}}$ if and only if there exists $m \in \mathsf{Spec}$ for which $\ell \owedge m$ and $\ell' \owedge m$ are defined.

The conjunction of two SMTS S, T is the SMTS $S \wedge T = \rho_B(S \times T, (s_0, t_0), \dashrightarrow_{S \wedge T}, \longrightarrow_{S \wedge T})$ given as follows:

$$\frac{s \overset{k}{\longrightarrow}_S s' \qquad t \overset{\ell}{\dashrightarrow}_T t' \qquad k \owedge \ell \text{ defined}}{(s,t) \overset{k \owedge \ell}{\longrightarrow}_{S \wedge T} (s',t')} \qquad \frac{s \overset{k}{\dashrightarrow}_S s' \qquad t \overset{\ell}{\longrightarrow}_T t' \qquad k \owedge \ell \text{ defined}}{(s,t) \overset{k \owedge \ell}{\longrightarrow}_{S \wedge T} (s',t')}$$

$$\frac{s \overset{k}{\dashrightarrow}_S s' \qquad t \overset{\ell}{\dashrightarrow}_T t' \qquad k \owedge \ell \text{ defined}}{(s,t) \overset{k \owedge \ell}{\dashrightarrow}_{S \wedge T} (s',t')}$$

$$\frac{s \overset{k}{\longrightarrow}_S s' \qquad \forall t \overset{\ell}{\dashrightarrow}_T t' : k \owedge \ell \text{ undefined}}{(s,t) \in B} \qquad \frac{t \overset{\ell}{\longrightarrow}_T t' \qquad \forall s \overset{k}{\dashrightarrow}_S s' : k \owedge \ell \text{ undefined}}{(s,t) \in B}$$

With this definition, it can be shown [5] that conjunction acts as *greatest lower bound*: Given SMTS S, T for which $S \wedge T$ is defined, we have $S \wedge T \leq_m S$ and $S \wedge T \leq_m T$, and if S or T is deterministic and U is a SMTS for which $U \leq_m S$ and $U \leq_m T$, then $S \wedge T$ is defined and $U \leq_m S \wedge T$. We again note that this property implies uniqueness, up to $\equiv_m$, of conjunction: if conjunction exists, it must be given as above.

To generalize this to a quantitative greatest lower bound property, we shall have reason to consider two different properties of the label operator $\oslash$. The first is analogous to the one for structural composition above: we say that $\oslash$ is *bounded* by a function $C : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ if C is monotone in both coordinates, has $C(\bot_{\mathbb{L}}, \bot_{\mathbb{L}}) = \bot_{\mathbb{L}}$, $C(\alpha, \top_{\mathbb{L}}) = C(\top_{\mathbb{L}}, \alpha) = \top_{\mathbb{L}}$ for all $\alpha \in \mathbb{L}$, and if it holds for all $k, \ell, m \in \mathsf{Spec}$ for which $d_T(m,k) \neq \infty$ and $d_T(m,\ell) \neq \infty$ that $k \oslash \ell$ is defined and

$$F(m, k \oslash \ell, C(\alpha, \alpha')) \sqsubseteq_{\mathbb{L}} C(F(m,k,\alpha), F(m,\ell,\alpha'))$$

for all $\alpha, \alpha' \in \mathbb{L}$. For such a bounded $\oslash$ it can be shown [4] that if S, T, U are SMTS of which S or T is deterministic, and if $h_m(U,S) \neq \top_{\mathbb{L}}$ and $h_m(U,T) \neq \top_{\mathbb{L}}$, then $S \wedge T$ is defined and $h_m(U, S \wedge T) \sqsubseteq_{\mathbb{L}} C(h_m(U,S), h_m(U,T))$.

For the second, *relaxed* boundedness property of $\oslash$, we have to first introduce a notion of *quantitative widening*. For $\alpha \in \mathbb{L}$ and SMTS S, T, we say that T is an α-*widening* of S if there is a relation $R \subseteq S \times T$ for which $(s_0, t_0) \in R$ and such that for all $(s,t) \in R$, $s \overset{k}{\dashrightarrow}_S s'$ if and only if $t \overset{\ell}{\dashrightarrow}_T t'$, and $s \xrightarrow{k}_S s'$ if and only if $t \xrightarrow{\ell}_T t'$, for $k \sqsubseteq_{\mathsf{Spec}} \ell$, $d(\ell, k) \sqsubseteq_{\mathbb{L}} \alpha$, and $(s', t') \in R$. Thus up to unweighted two-sided refinement, T is the same as S, but transition labels in T can be α "wider" than in S. (Hence also $S \leq_m T$, but nothing general can be said about quantitative refinement from T to S, *cf.* [4].)

We say that the operator $\oslash$ is *relaxed bounded* by a function family $C = \{C_{\beta,\gamma} : \mathbb{L} \times \mathbb{L} \to \mathbb{L} \mid \beta, \gamma \in \mathbb{L}\}$ if all $C_{\beta,\gamma}$ are monotone in both coordinates, have $C_{\beta,\gamma}(\bot_{\mathbb{L}}, \bot_{\mathbb{L}}) = \bot_{\mathbb{L}}$, $C_{\beta,\gamma}(\alpha, \top_{\mathbb{L}}) = C_{\beta,\gamma}(\top_{\mathbb{L}}, \alpha) = \top_{\mathbb{L}}$ for all $\alpha \in \mathbb{L}$, and if it holds for all $k, \ell \in \mathsf{Spec}$ for which there is $m \in \mathsf{Spec}$ with $h_T(m,k) \neq \top_{\mathbb{L}}$ and $h_T(m,\ell) \neq \top_{\mathbb{L}}$ that there exist $k', \ell' \in \mathsf{Spec}$ with $k \sqsubseteq_{\mathsf{Spec}} k'$, $\ell \sqsubseteq_{\mathsf{Spec}} \ell'$, $h_T(k',k) = \beta \neq \top_{\mathbb{L}}$, and $h_T(\ell',\ell) = \gamma \neq \top_{\mathbb{L}}$, such that $k' \oslash \ell'$ is defined, and then for all $m \in \mathsf{Spec}$ with $h_T(m,k) \neq \top_{\mathbb{L}}$ and $d_T(m,\ell) \neq \top_{\mathbb{L}}$,

$$F(m, k' \oslash \ell', C_{\beta,\gamma}(\alpha, \alpha')) \sqsubseteq_{\mathbb{L}} C_{\beta,\gamma}(F(m,k,\alpha), F(m,\ell,\alpha'))$$

for all $\alpha, \alpha' \in \mathbb{L}$. The following property can then be shown [4, Thm. 5]: Let S, T be SMTS with S or T deterministic. If there is an SMTS U for which $h_m(U,S) \neq \top_{\mathbb{L}}$ and $h_m(U,T) \neq \top_{\mathbb{L}}$, then there exist β- and γ-widenings S' of S and T' of T for which $S' \wedge T'$ is defined, and such that $h_m(U, S' \wedge T') \sqsubseteq_{\mathbb{L}} C_{\beta,\gamma}(h_m(U,S), h_m(U,T))$ for all SMTS U for which $h_m(U,S) \neq \top_{\mathbb{L}}$ and $h_m(U,T) \neq \top_{\mathbb{L}}$.

3 Robust Semantics of Modal Event-Clock Specifications

As an application of the framework laid out in this paper, we consider the modal event-clock specifications (MECS) of [7] and give them a robust semantics as SMTS. We choose MECS instead of a more expressive real-time formalism such as *e.g.* timed automata [1] mainly for ease of exposition; it is certainly possible to extend the work presented here also to these formalisms.

We assume a fixed finite alphabet Σ and let $\delta \notin \Sigma$ denote a special symbol which signifies passage of time. Let $\Phi(\Sigma)$ denote the set of closed clock constraints over Σ, given by

$$\Phi(\Sigma) \ni \phi ::= a \leq k \mid a \geq k \mid \phi_1 \wedge \phi_2 \qquad (a \in \Sigma, k \in \mathbb{N}, \phi_1, \phi_2 \in \Phi(\Sigma)).$$

A (real) clock valuation is a mapping $u : \Sigma \to \mathbb{R}_{\geq 0}$; we say that $u \models \phi$, for $\phi \in \Phi(\Sigma)$, if $u(a)$ satisfies ϕ for all $a \in \Sigma$, and we let $[\![\phi]\!] = \{u : \Sigma \to \mathbb{R}_{\geq 0} \mid u \models \phi\}$. For $d \in \mathbb{R}_{\geq 0}$ and $b \in \Sigma$ we define the valuations $u + d = \lambda a.(u(a) + d)$ and $u[b] = \lambda a.(\text{if } a = b \text{ then } 0 \text{ else } u(a))$. Note that for brevity we use lambda notation for anonymous functions here.

We denote by $\mathbb{I} = \{[x,y] \mid x \in \mathbb{R}_{\geq 0}, y \in \mathbb{R}_{\geq 0} \cup \{\infty\}, x \leq y\}$ the set of closed extended non-negative real intervals, and define addition of intervals by $[l,r] + [l',r'] = [l+l', r+r']$. An *interval clock valuation* is a mapping $v : \Sigma \to \mathbb{I}$ associating with each symbol a a non-negative interval $v(a) = [l_a, r_a] \in \mathbb{I}$ of possible clock values. We say that $v \models \phi$, for $\phi \in \Phi(\Sigma)$, if there exists $u : \Sigma \to \mathbb{R}_{\geq 0}$ for which $u(a) \in v(a)$ for all $a \in \Sigma$ and $u \models \phi$. For $d \in \mathbb{I}$ and $b \in \Sigma$ we define $v + d = \lambda a.(v(a) + [d,d])$ and $u[b] = \lambda a.(\text{if } a = b \text{ then } [0,0] \text{ else } u(a))$.

A *modal event-clock specification* (MECS) [7] is a tuple $A = (Q, q_0, \dashrightarrow_A, \longrightarrow_A)$ consisting of a finite set Q of locations, with initial location $q_0 \in Q$, and *may* and *must* edges $\dashrightarrow_A, \longrightarrow_A \subseteq Q \times \Sigma \times \Phi(\Sigma) \times Q$ which satisfy that for all $(q,a,g,q') \in \longrightarrow_A$ there exists $(q,a,g',q') \in \dashrightarrow_A$ with $[\![g]\!] \subseteq [\![g']\!]$. As before we write $q \overset{a,g}{\dashrightarrow}_A q'$ instead of $(q,a,g,q') \in \dashrightarrow_A$, similarly for $\longrightarrow_A$. Figure 1 shows some examples of MECS.

To facilitate robust analysis of MECS, we give their semantics not as usual timed transition systems [1] (or as modal region automata as in [7]), but as *interval timed modal transition systems* (ITMTS). These are SMTS over

$$\mathsf{Spec} = (\Sigma \times \{[0,0]\}) \cup (\{\delta\} \times \mathbb{I}) \subseteq (\Sigma \cup \{\delta\}) \times \mathbb{I},$$

with $(a,[l,r]) \sqsubseteq_{\mathsf{Spec}} (a',[l',r'])$ if and only if $a = a'$, $l \geq l'$, and $r \leq r'$ (hence $[l,r] \subseteq [l',r']$), and thus with $\mathsf{Imp} = \Sigma \times \{0\} \cup \{\delta\} \times \mathbb{R}_{\geq 0}$. Hence an implementation is a usual timed transition system, with discrete transitions $s \xrightarrow{a,0} s'$ and delay transitions $s \xrightarrow{\delta,d} s'$.

The *semantics* of a MECS $A = (Q, q_0, \dashrightarrow_A, \longrightarrow_A)$ is the ITMTS $(\!|A|\!) = (S, s_0, \dashrightarrow_S, \longrightarrow_S)$ given as follows:

$$\begin{aligned}
S &= \{(q,v) \mid q \in Q, v : \Sigma \to \mathbb{I}\} \qquad s_0 = (q_0, \lambda x.0) \\
\longrightarrow_S &= \{(q,v) \xrightarrow{a,0}_S (q',v') \mid q \xrightarrow{a,g}_A q', v \models g, v' = v[a]\} \cup \{(q,v) \xrightarrow{\delta,[l,r]}_S (q,v') \mid v' = v + [l,r]\} \\
\dashrightarrow_S &= \{(q,v) \overset{a,0}{\dashrightarrow}_S (q',v') \mid q \overset{a,g}{\dashrightarrow}_A q', v \models g, v' = v[a]\} \cup \{(q,v) \overset{\delta,[l,r]}{\dashrightarrow}_S (q,v') \mid v' = v + [l,r]\}
\end{aligned}$$

Note that the "real", precise semantics of A as a timed transition system [1] is an implementation of $(\!|A|\!)$, also any of the "relaxed" or "robust" semantics of [8, 17, 24, 25] are implementations of $(\!|A|\!)$; any robust semantics "lives" in our framework. As we are using closed clock constraints for MECS, $(\!|A|\!)$ as defined above is compactly branching.

Refinement of MECS is defined semantically: $A \leq_m B$ if $(\!|A|\!) \leq_m (\!|B|\!)$. Note that the refinement of [7] is different (indeed it is not quantitative in our sense). By definition of modal refinement, a specification $S \leq_m (\!|A|\!)$ is a *more precise*, or less relaxed, specification of the semantics of A: any delay intervals on transitions $s \overset{\delta,[l,r]}{\dashrightarrow}_S s'$ are contained in intervals $t \overset{\delta,[l',r']}{\dashrightarrow}_{(\!|A|\!)} t'$ (and similarly for *must* transitions).

We are interested in *timing differences* of (refinements of) MECS, *i.e.* in expressing how much two ITMTS can differ in the timings of their behaviors. Given two finite traces $\sigma = (a_0,x_0), \dots, (a_n,x_n)$ and $\sigma' = (a_0,x'_0), \dots, (a_n,x'_n)$ (note that the discrete labels in $\Sigma \cup \{\delta\}$ are the same), their timing difference is $|(x_0 + x_1 + \cdots + x_n) - (x'_0 + x'_1 + \cdots + x'_n)|$, and what interests us is the *maximal* timing difference at any point of the runs. Hence we want the distance between σ and σ' to be $\max_{m=0,\dots,n} |\sum_{i=0}^m x_i - \sum_{i=0}^m x'_i|$, and

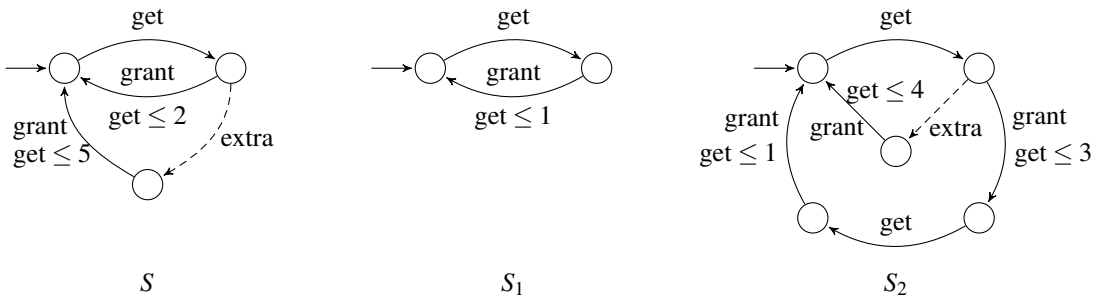

Figure 1: An MECS model S of a resource specification, *cf.* [7], and two refinement candidates S_1, S_2. As customary, we omit *may*-transitions which have an underlying *must*-transition with the same label. Note that $S_1 \leq_m S$ and $S_2 \not\leq_m S$, but $d_m(S_2, S) = 1$.

with the $\max_{m=0,\ldots,n}$ replaced by $\sup_{m\in\mathbb{N}}$ for infinite traces. This is precisely the *maximum-lead distance* of [18, 26], and we show below how it fits in the framework of this paper.

Note that the accumulating distance of [3] measures something entirely different: for the finite traces above, it is $|x_0 - x'_0| + \lambda|x_1 - x'_1| + \cdots + \lambda^n|x_n - x'_n|$, hence measuring the sum of the differences in the individual timings of transitions rather than the overall timing difference. Thus the work laid out in [3] is not applicable to our setting, showing the strength of the more general approach of [4].

Let $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^{\mathbb{R}}$, the set of mappings from *leads* to distances, define $F : \mathsf{Imp} \times \mathsf{Imp} \times \mathbb{L} \to \mathbb{L}$ by

$$F((a,t),(a',t'),\alpha) = \begin{cases} \top_{\mathbb{L}} & \text{if } a \neq a', \\ \lambda d.\max(|d+t-t'|, \alpha(d+t-t')) & \text{if } a = a' \end{cases}$$

and extend F to specifications by $F(k,\ell,\alpha) = \sup_{m\in[\![k]\!]} \inf_{n\in[\![\ell]\!]} F(m,n,\alpha)$. Define $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ by $g(\alpha) = \alpha(0)$; the maximum-lead distance assuming the lead is zero. Using our characterization of h_T from (1), it can then be shown that $d_T = g \circ h_T : \mathsf{Spec}^\infty \times \mathsf{Spec}^\infty \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ is precisely the maximum-lead distance, *cf.* [13, 18]. We also instantiate our definitions of modal and thorough refinement distance for ITMTS; for MECS A, B we let $d_m(A,B) = d_m(\langle\!|A|\!\rangle, \langle\!|B|\!\rangle)$, $d_t(A,B) = d_t(\langle\!|A|\!\rangle, \langle\!|B|\!\rangle)$.

Determinism for ITMTS is the same as in [3]: if $k_1, k_2 \in \mathsf{Spec}$, with $k_1 = (a_1, [l_1, r_1])$, $k_2 = (a_2, [l_2, r_2])$, then there is $k \in \mathsf{Spec}$ with $h_T(k,k_1) \neq \top_{\mathbb{L}}$ and $h_T(k,k_2) \neq \top_{\mathbb{L}}$ if and only if $a_1 = a_2$. Hence an ITMTS S is deterministic if and only if it holds for all $s \in S$ that $s \overset{(a,[l_1,r_1])}{\dashrightarrow}_S s_1$ and $s \overset{(a,[l_2,r_2])}{\dashrightarrow}_S s_2$ imply $[l_1,r_1] = [l_2,r_2]$ and $s_1 = s_2$. For an MECS A, $\langle\!|A|\!\rangle$ is hence deterministic if and only if for all locations q, $q \overset{a,g_1}{\dashrightarrow} q_1$ and $q \overset{a,g_2}{\dashrightarrow} q_2$ imply that $[\![g_1]\!] = [\![g_2]\!]$ and $q_1 = q_2$. This is a stronger notion of determinism than in [7]; we will call it *strong determinism* for differentiation.

For *structural composition* of ITMTS we use CSP-style synchronization on discrete labels and intersection of intervals. Note that this is different from [3] which instead uses addition of intervals. Given $(a,[l,r]), (a',[l',r']) \in \mathsf{Spec}$ we hence define

$$(a,[l,r]) \oplus (a',[l',r']) = \begin{cases} (a,[\max(l,l'),\min(r,r')]) & \text{if } a = a' \text{ and } \max(l,l') \leq \min(r,r'), \\ \text{undefined} & \text{otherwise}. \end{cases}$$

It can be shown that $\oplus$ is bounded by $P(\alpha,\alpha') = \max(\alpha,\alpha')$. Also, the notion of structural composition of ITMTS we obtain is consistent with the one of synchronized product of [7] (denoted $\otimes$ in that paper). Figure 2 depicts some examples of structural compositions.

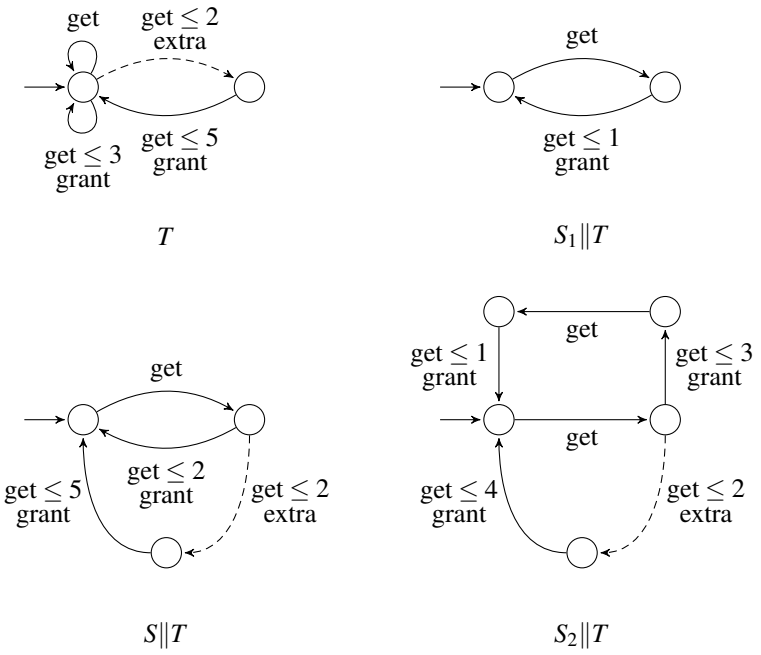

Figure 2: A MECS model T of a process accessing the resource S from Fig. 1, together with the structural compositions $S\|T$, $S_1\|T$, and $S_2\|T$. Note that $d_m(S_2\|T, S\|T) = 1$.

Theorem 1. *Let A, B, A', B' be MECS. With $\|$ the notion of synchronized product of MECS from [7], $(\!|A\|B|\!) \equiv_m (\!|A|\!)\|(\!|B|\!)$. Additionally, $d_m(A\|A', B\|B') \leq \max(d_m(A,B), d_m(A',B'))$.*

Proof. $(\!|A\|B|\!) \equiv_m (\!|A|\!)\|(\!|B|\!)$ is clear from the definitions. For the second part, we have $h_m(A\|A', B\|B') \sqsubseteq_{\mathbb{L}} P(h_m(A,B), h_m(A',B')) = \max(h_m(A,B), h_m(A',B'))$ by [4, Thm. 2], and as $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ is a homomorphism, the claim follows. □

For *quotient* of ITMTS we define, for labels $(a,[l,r]), (a',[l',r']) \in \mathsf{Spec}$,

$$(a',[l',r']) \oslash (a,[l,r]) = \begin{cases} \text{undefined} & \text{if } a \neq a', \\ (a,[l',\infty]) & \text{if } a = a' \text{ and } l < l' \leq r \leq r', \\ (a,[l',r']) & \text{if } a = a' \text{ and } l < l' \leq r' < r, \\ \text{undefined} & \text{if } a = a' \text{ and } l \leq r < l' \leq r', \\ (a,[0,\infty]) & \text{if } a = a' \text{ and } l' \leq l \leq r \leq r', \\ (a,[0,r']) & \text{if } a = a' \text{ and } l' \leq l \leq r < r', \\ \text{undefined} & \text{if } a = a' \text{ and } l' \leq r' < l \leq r. \end{cases}$$

The intuition is that to obtain the maximal solution $[p,q]$ to an equation $[l,r] \oplus [p,q] \sqsubseteq_{\mathsf{Spec}} [l',r']$, whether p and q must restrain the interval in the intersection, or can be 0 and ∞, respectively, depends on the position of $[l,r]$ relative to $[l',r']$, *cf.* Figure 3. It can be shown that the operator $\oslash$ is quantitatively well-behaved.

We can lift our quotient from the semantic ITMTS level to MECS as follows: A clock constraint in $\Phi(\Sigma)$ is equivalent to a mapping $\Sigma \to \mathbb{J}$, where $\mathbb{J} = \{[x,y] \mid x \in \mathbb{N}, y \in \mathbb{N} \cup \{\infty\}, x \leq y\} \subseteq \mathbb{I}$ denotes the set of closed extended non-negative integer intervals, and then we can define $\phi' \oslash \phi = \lambda a.(\phi'(a) \oslash \phi(a))$

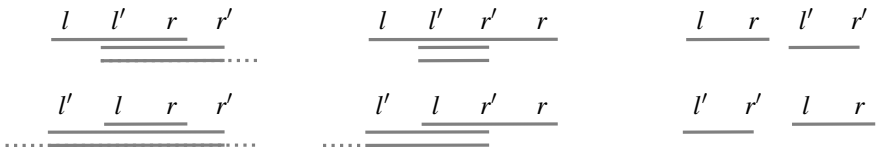

Figure 3: Quotient $[l',r'] \oslash [l,r]$ of intervals, six cases. Top bar: $[l,r]$; middle bar: $[l',r']$; bottom bar: quotient. Note that for the two cases on the right, quotient is undefined.

with $\oslash$ defined on intervals as above. Our quotient of MECS is then defined as in [7], but with their guard operation replaced by our $\oslash$ (hence our quotient is different from theirs, which is to be expected as the notions of refinement are different).

Theorem 2. *Let A, B, X be MECS for which $B \mathbin{\backslash\!\backslash} A$ exists, then $(\!|B \mathbin{\backslash\!\backslash} A|\!) \equiv (\!|B|\!) \mathbin{\backslash\!\backslash} (\!|A|\!)$. If A is strongly deterministic, then $d_m(X, B \mathbin{\backslash\!\backslash} A) \leq d_m(A\|X, B)$, and $X \leq_m B \mathbin{\backslash\!\backslash} A$ if and only if $A\|X \leq_m B$.*

Proof. $(\!|B \mathbin{\backslash\!\backslash} A|\!) \equiv (\!|B|\!) \mathbin{\backslash\!\backslash} (\!|A|\!)$ is clear from the definitions. For the second part, $X \leq_m B \mathbin{\backslash\!\backslash} A$ if and only if $A\|X \leq_m B$ by [4, Thm. 3], and by the same theorem, $h_m(X, B \mathbin{\backslash\!\backslash} A) \sqsubseteq h_m(A\|X, B)$, so as $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$, the claim follows. □

The *conjunction* operator on labels of ITMTS is defined using intersection of intervals like for structural composition, hence we let $k \mathbin{\mathbb{O}} \ell = k \mathbin{\mathbb{O}} \ell$ for $k, \ell \in \mathsf{Spec}$. The intuition is that transition intervals give constraints on timings; hence a synchronized transition has to satisfy both interval constraints. It can be shown that $\mathbb{O}$ is *not* bounded, but relaxed bounded by $C_{\beta,\gamma}(\alpha,\alpha') = \max(\alpha,\alpha') \oplus_{\mathbb{L}} \max(\beta,\gamma)$.

Our notion of conjunction is consistent with the one for MECS in [7], and to make use of relaxed boundedness, we need to lift the notion of quantitative widening from the semantic ITMTS level to MECS. This is done by defining, for a clock constraint $\phi : \Sigma \to \mathbb{J}$ and $n \in \mathbb{N}$, the n-extended constraint $\phi_{+n} = \lambda a.\phi(a) + [-n,n]$ (this is similar to a construction in [8]), and then saying that a MECS B is an n-widening of an MECS A if there is a relation $R \subseteq Q_A \times Q_B$ for which $(q_0^A, q_0^B) \in R$, and for all $(q_A, q_B) \in R$, $q_A \overset{a,g}{\dashrightarrow}_A q'_A$ if and only if $q_B \overset{a,g+n}{\dashrightarrow} q'_B$ with $(q_B, q'_B) \in R$ and similarly for *must* transitions.

Theorem 3. *Let A, B be MECS. With $\wedge$ the notion of greatest lower bound from [7], $(\!|A \wedge B|\!) \equiv (\!|A|\!) \wedge (\!|B|\!)$. If A or B is strongly deterministic and there is a MECS C for which $d_m(C,A) \neq \infty$ and $d_m(C,B) \neq \infty$, then there are an n-widening A' of A and an m-widening B' of B for which $A' \wedge B'$ is defined, and such that $d_m(C, A' \wedge B') \leq \max(d_m(C,A), d_m(C,B)) + \max(n,m)$ for all MECS C for which $d_m(C,A) \neq \infty$ and $d_m(C,B) \neq \infty$.*

Proof. $(\!|A \wedge B|\!) \equiv (\!|A|\!) \wedge (\!|B|\!)$ by definition, and the second claim follows from [4, Thm. 5] and the homomorphism property of $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$. □

References

[1] Rajeev Alur & David Dill (1994): *A Theory of Timed Automata*. *Theoretical Computer Science* 126(2), pp. 183–235. Available at `http://dx.doi.org/10.1016/0304-3975(94)90010-8`.

[2] Sebastian S. Bauer, Alexandre David, Rolf Hennicker, Kim G. Larsen, Axel Legay, Ulrik Nyman & Andrzej Wasowski (2012): *Moving from Specifications to Contracts in Component-Based Design*. In Juan de Lara & Andrea Zisman, editors: *FASE*, *Lecture Notes in Computer Science* 7212, Springer-Verlag, pp. 43–58. Available at `http://dx.doi.org/10.1007/978-3-642-28872-2_3`.

[3] Sebastian S. Bauer, Uli Fahrenberg, Line Juhl, Kim G. Larsen, Axel Legay & Claus R. Thrane (2011): *Quantitative Refinement for Weighted Modal Transition Systems*. In Filip Murlak & Piotr Sankowski, editors: *MFCS*, *Lecture Notes in Computer Science* 6907, Springer-Verlag, pp. 60–71. Available at `http://dx.doi.org/10.1007/978-3-642-22993-0_9`.

[4] Sebastian S. Bauer, Uli Fahrenberg, Axel Legay & Claus Thrane (2012): *General Quantitative Specification Theories with Modalities*. In: *CSR*, *Lecture Notes in Computer Science* 7353, Springer-Verlag. To appear.

[5] Sebastian S. Bauer, Line Juhl, Kim G. Larsen, Axel Legay & Jiří Srba (2012): *Extending Modal Transition Systems with Structured Labels*. *Mathematical Structures in Computer Science*. To appear.

[6] Nikola Beneš, Jan Křetínský, Kim G. Larsen & Jirí Srba (2009): *Checking Thorough Refinement on Modal Transition Systems Is EXPTIME-Complete*. In Martin Leucker & Carroll Morgan, editors: *ICTAC*, *Lecture Notes in Computer Science* 5684, Springer-Verlag, pp. 112–126. Available at `http://dx.doi.org/10.1007/978-3-642-03466-4_7`.

[7] Nathalie Bertrand, Axel Legay, Sophie Pinchinat & Jean-Baptiste Raclet (2009): *A Compositional Approach on Modal Specifications for Timed Systems*. In Karin Breitman & Ana Cavalcanti, editors: *ICFEM*, *Lecture Notes in Computer Science* 5885, Springer-Verlag, pp. 679–697. Available at `http://dx.doi.org/10.1007/978-3-642-10373-5_35`.

[8] Patricia Bouyer, Kim G. Larsen, Nicolas Markey, Ocan Sankur & Claus R. Thrane (2011): *Timed Automata Can Always Be Made Implementable*. In Joost-Pieter Katoen & Barbara König, editors: *CONCUR*, *Lecture Notes in Computer Science* 6901, Springer-Verlag, pp. 76–91. Available at `http://dx.doi.org/10.1007/978-3-642-23217-6_6`.

[9] Franck van Breugel (1996): *A Theory of Metric Labelled Transition Systems*. *Annals of the New York Academy of Sciences* 806(1), pp. 69–87. Available at `http://dx.doi.org/10.1111/j.1749-6632.1996.tb49160.x`.

[10] Uli Fahrenberg, Kim G. Larsen & Claus Thrane (2010): *A Quantitative Characterization of Weighted Kripke Structures in Temporal Logic*. *Comp. Inf.* 29(6+), pp. 1311–1324.

[11] Uli Fahrenberg, Axel Legay & Claus Thrane (2011): *The Quantitative Linear-Time–Branching-Time Spectrum*. In Supratik Chakraborty & Amit Kumar, editors: *FSTTCS*, *LIPIcs* 13, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, pp. 103–114. Available at `http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2011.103`.

[12] Uli Fahrenberg, Axel Legay & Andrzej Wasowski (2011): *Make a Difference! (Semantically)*. In Jon Whittle, Tony Clark & Thomas Kühne, editors: *MoDELS*, *Lecture Notes in Computer Science* 6981, Springer-Verlag, pp. 490–500. Available at `http://dx.doi.org/10.1007/978-3-642-24485-8_36`.

[13] Uli Fahrenberg, Claus R. Thrane & Kim G. Larsen (2011): *Distances for Weighted Transition Systems: Games and Properties*. In Mieke Massink & Gethin Norman, editors: *QAPL*, *Electronic Proceedings in Theoretical Computer Science* 57, pp. 134–147. Available at `http://dx.doi.org/10.4204/EPTCS.57.10`.

[14] Patrice Godefroid, Michael Huth & Radha Jagadeesan (2001): *Abstraction-Based Model Checking Using Modal Transition Systems*. In Kim Guldstrand Larsen & Mogens Nielsen, editors: *CONCUR*, *Lecture Notes in Computer Science* 2154, Springer-Verlag, pp. 426–440. Available at `http://dx.doi.org/10.1007/3-540-44685-0_29`.

[15] Alexander Gruler, Martin Leucker & Kathrin D. Scheidemann (2008): *Modeling and Model Checking Software Product Lines*. In Gilles Barthe & Frank S. de Boer, editors: *FMOODS*, *Lecture Notes in Computer Science* 5051, Springer-Verlag, pp. 113–131. Available at `http://dx.doi.org/10.1007/978-3-540-68863-1_8`.

[16] Orna Grumberg, Martin Lange, Martin Leucker & Sharon Shoham (2005): *Don't Know in the μ-calculus*. In Radhia Cousot, editor: *VMCAI*, *Lecture Notes in Computer Science* 3385, Springer-Verlag, pp. 233–249. Available at `http://dx.doi.org/10.1007/978-3-540-30579-8_16`.

[17] Vineet Gupta, Thomas A. Henzinger & Radha Jagadeesan (1997): *Robust Timed Automata*. In Oded Maler, editor: *HART*, *Lecture Notes in Computer Science* 1201, Springer-Verlag, pp. 331–345. Available at http://dx.doi.org/10.1007/BFb0014736.

[18] Thomas A. Henzinger, Rupak Majumdar & Vinayak S. Prabhu (2005): *Quantifying Similarities Between Timed Systems*. In Paul Pettersson & Wang Yi, editors: *FORMATS*, *Lecture Notes in Computer Science* 3829, Springer-Verlag, pp. 226–241. Available at http://dx.doi.org/10.1007/11603009_18.

[19] Kim G. Larsen (1989): *Modal Specifications*. In: *Automatic Verification Methods for Finite State Systems*, *Lecture Notes in Computer Science* 407, Springer-Verlag, pp. 232–246. Available at http://dx.doi.org/10.1007/3-540-52148-8_19.

[20] Kim G. Larsen, Uli Fahrenberg & Claus R. Thrane (2011): *Metrics for weighted transition systems: Axiomatization and complexity*. *Theoretical Computer Science* 412(28), pp. 3358–3369. Available at http://dx.doi.org/10.1016/j.tcs.2011.04.003.

[21] James R. Munkres (2000): *Topology*. Prentice Hall.

[22] Ulrik Nyman (2008): *Modal Transition Systems as the Basis for Interface Theories and Product Lines*. Ph.D. thesis, Aalborg University.

[23] Mathieu Sassolas, Marsha Chechik & Sebastián Uchitel (2011): *Exploring inconsistencies between modal transition systems*. *Software and System Modeling* 10(1), pp. 117–142. Available at http://dx.doi.org/10.1007/s10270-010-0148-x.

[24] Mani Swaminathan & Martin Fränzle (2007): *A Symbolic Decision Procedure for Robust Safety of Timed Systems*. In: *TIME*, IEEE Computer Society, p. 192. Available at http://doi.ieeecomputersociety.org/10.1109/TIME.2007.39.

[25] Mani Swaminathan, Martin Fränzle & Joost-Pieter Katoen (2008): *The Surprising Robustness of (Closed) Timed Automata against Clock-Drift*. In Giorgio Ausiello, Juhani Karhumäki, Giancarlo Mauri & C.-H. Luke Ong, editors: *IFIP TCS*, *IFIP* 273, Springer-Verlag, pp. 537–553. Available at http://dx.doi.org/10.1007/978-0-387-09680-3_36.

[26] Claus Thrane, Uli Fahrenberg & Kim G. Larsen (2010): *Quantitative Simulations of Weighted Transition Systems*. *Journal of Logic and Algebraic Programming* 79(7), pp. 689–703. Available at http://dx.doi.org/10.1016/j.jlap.2010.07.010.